Communications Security Establishment Commissioner

Annual Report

2002 ↓ 2003

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2003
ISBN 0-662-67417-0
Cat. No. D95-2003

Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

June 2003

The Honourable John McCallum, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. McCallum:

Pursuant to sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2002-2003 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

Introduction 1

The Evolving Role of the Commissioner 2

2002-2003 Activities 4

- Classified Reports 4
- Reviews of Activities under Ministerial Authorizations 5
- Other Reviews 7
- 2002-03 Findings 9
- Complaints and Concerns about CSE Activities 10
- Review Agencies Conference 10

The Commissioner's Office 11

- Office Expenditures and Staff 11
- Accommodation 11

Looking Ahead 11

- The Public Safety Act 11
- Appointment of a New Commissioner 12
- Concluding Thoughts 13

Annex A: Commissioner's Mandate 15

Annex B: Budget and Expenditures 2002-03 17

Annex C: Classified Reports, 1996-2003 19

INTRODUCTION

This is my seventh and final report as Commissioner of the Communications Security Establishment (CSE), as my appointment will terminate in June 2003. It is also the first time since my initial appointment in 1996 that my review of CSE's activities and my annual report have been guided by legislation.

In my last report I pointed out that after more than a decade of debate about the pros and cons of enabling legislation for CSE, the tragic events of 11 September 2001 precipitated the introduction and passage of the omnibus *Anti-Terrorism Act* by Parliament. The resulting amendments to the *National Defence Act,* which came into effect on 24 December 2001, created a legislated mandate for CSE as well as for the CSE Commissioner. The new provisions of the *National Defence Act* enshrined in legislation the historical activities of CSE as well as the activities I had been carrying out since 1996, but they also introduced new elements. These are described more fully in the next section.

Much of this past year has been taken up with assessing the implications of my new duties and making a start on meeting the requirements of the legislation. As a result, it has been a year of much challenge and change for both CSE and my Office as we move toward a common understanding of our respective roles and responsibilities.

In this year's annual report I look back briefly on seven years of evolution and development in the Commissioner's role. I also report on the review activities and findings of my Office in 2002-03. These addressed CSE's two main programs (Signals Intelligence and Information Technology Security) as well as some of its other activities. Finally, I look forward to developments that are already on the horizon and to the appointment of my successor.

THE EVOLVING ROLE OF THE COMMISSIONER

Since I started as Commissioner in 1996, the highly complex environment in which CSE works has changed dramatically. So has the work of my Office and the expectations placed upon it.

One aspect of the change results from the technology-rich environment within which CSE works – and the technology involved has been advancing at an accelerating pace throughout this time. Another key element relates to changes in the intelligence environment that derive from evolving political, social and economic realities. These have led to new threats to Canada's security, defence and national interests and changes to the government's intelligence priorities. To address these challenges, CSE has expanded its role in the collection, analysis and reporting of information and intelligence. My staff and I have had to learn about the complex technologies involved and to stay on top of the rapid changes taking place in order to carry out the Commissioner's review role effectively and efficiently.

Throughout this period of dynamic change in technology, in the intelligence environment, and in CSE's activities, I have been guided by the principle that Canadians deserve the assurance that CSE, which must of necessity conduct most of its business in secret, does so in compliance with the laws of Canada. Providing this assurance has been my responsibility, and I have sought to fulfil it by maintaining the breadth, depth and credibility of my Office's review work, with a particular focus on those matters that could put the privacy of Canadians at risk.

The Commissioner's role, as it had developed under mandates set out in the June 1996 and June 1999 Orders in Council appointing me Commissioner, was confirmed and extended by Parliament in the *Anti-Terrorism Act* of December 2001. The most significant extension of my role arises from

provisions that allow the Minister of National Defence to authorize CSE's interception of the private communications of Canadians in specific circumstances and subject to several conditions set out in the legislation.[1] Section 183 of the *Criminal Code* defines private communications as

> ...any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada, and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it...

This new power of CSE to intercept private communications when authorized by the Minister is a significant development, bringing with it obvious risks to the privacy of Canadians. These risks are recognized in the legislation, which requires, among other things, that the Minister be satisfied that CSE has satisfactory measures in place to protect the privacy of Canadians. In addition, the legislation directs the Commissioner to review activities carried out under each ministerial authorization to ensure that they are indeed authorized, and to report annually to the Minister on the review. Based on experience to date, I anticipate that this will be a substantial and challenging aspect of the Commissioner's role in the future.

A further extension to the Commissioner's role was set out in the *Security of Information Act* (the former *Official Secrets Act*). This Act prohibits people bound by secrecy from communicating or confirming "special operational information", including special operational information about

[1] Before December 2001, CSE would have been in violation of privacy-related provisions of both the *Criminal Code* and the *Canadian Charter of Rights and Freedoms* had it intercepted communications without the certainty that, in doing so, it would not intercept private communications.

CSE's activities. A person would not be found guilty of an offence, however, if that person could establish that he or she acted in the public interest. A judge can consider a "public interest defence" only if the person involved has taken a series of steps set out in the legislation before disclosing the information. These steps may include bringing concerns about CSE's activities to the Commissioner and allowing a reasonable time for the Commissioner to respond. Although I am hopeful that this role will rarely be exercised, it is potentially an important one and is likely to be demanding when a concern is brought to the Commissioner's attention.

The legislative provisions setting out the mandate of the Commissioner of the Communications Security Establishment are included in Annex A.

2002-03 ACTIVITIES

Classified Reports

Under the Orders in Council that set out my mandate from 19 June 1996 until 24 December 2001, my Office carried out a planned series of reviews of CSE's activities each year. These reviews were directed at areas where, in my opinion, the very nature of CSE's activities gave rise to risks relating to lawfulness. Because I was authorized to submit reports containing classified material to the Minister of National Defence at any time I considered advisable, I made it a practice to report the results of each of my reviews to the Minister in the form of a classified report.

The new legislation has introduced some important changes to my mandate. As described above, the Minister of National Defence may now authorize CSE to intercept the private communications of Canadians in some circumstances. Although I am still required to review CSE's activities generally to ensure that they are in compliance with the law, the legislation also directs me specifically to review CSE activities carried out under a ministerial

authorization to ensure they are authorized, and to report annually to the Minister on the review.

In other words, I no longer have a completely free hand in choosing subjects for review. Nor does my new legislated mandate specifically authorize me to submit reports containing classified material to the Minister whenever I consider it advisable. Nevertheless, in cases where I do choose the subjects for review, I believe it is sensible to continue the reporting practices established under my earlier mandate, as they have served well in the past.

During 2002-03 I forwarded four classified reports to the Minister, and another was nearing completion at the end of the year. These included reports mandated under the new legislation as well as reports on reviews of my own choosing. Annex C provides a list of all my classified reports to the Minister since my appointment in 1996.

As I have pointed out in the past, submitting a classified report to the Minister does not mean that I have identified any lack of compliance with the law or ministerial authority. It indicates only that the report contains material that requires classified handling. Indeed, I am pleased to say that none of the reviews on which my 23 classified reports are based (including the four reviews completed in 2002-03) identified incidents of unlawfulness or unauthorized activity.

Reviews of Activities under Ministerial Authorizations

Under sub-sections 273.65 (1) and (3) of the *National Defence Act*, the Minister of National Defence has authorized CSE, in writing, to intercept private communications for the purposes of obtaining foreign intelligence and protecting the computer systems or networks of the government from mischief, unauthorized use or interference. Because many of the activities carried out under

these authorizations were new to CSE, they gave rise to significant challenges relating not only to technology, but also to such matters as determining appropriate roles and responsibilities, developing policy and procedures to guide activities, and designing controls to ensure compliance with the conditions imposed by the legislation and the ministerial authorizations. CSE continues to address these challenges.

Information obtained from CSE indicates that the bulk of the communications intercepted under these authorizations are not in fact private communications (that is, they are not the communications of Canadians). Nevertheless, I believe that the unique focus of my review must be on private communications. Whatever else CSE may intercept, it is the interception of private communications that is specifically authorized by the Minister. Moreover, it is with respect to the interception, use and retention of private communications that issues of lawfulness and compliance with ministerial authority are most likely to arise. As a result, my Office devoted a significant part of its efforts during the past year to learning how CSE is acquiring, identifying, accessing, retaining and using such communications, as well as what kind of policy regime, procedures and management control framework it is putting in place. In doing so, my staff and I examined a variety of documents and correspondence, had several discussions with CSE officials, and attended briefings and information sessions. In addition, I asked CSE to take me through a specific tasking under one of the authorizations.

My Office completed a preliminary review of activities under one ministerial authorization. This authorized CSE to conduct activities from Canada relating to the interception of communications for the sole purpose of obtaining foreign intelligence

and, in doing so, to intercept private communications subject to conditions defined in the legislation and in the ministerial authorization. As required by the legislation, I reported the findings of this preliminary review to the Minister. Because of the focus of the ministerial authorization, and because the review was a first for my Office, my preliminary report related more to process and to the class of activities authorized than to CSE's compliance with authority. I anticipate that in future annual reports to the Minister under paragraph 273.65 of Part V.1 of the *National Defence Act,* the Commissioner will be in a position to address compliance issues more directly.

My reviews of activities under other ministerial authorizations in effect during 2002-03 were continuing at the end of the year and will be the subject of reports to the Minister in the near future.

Other Reviews

CSE's operational support to the Canadian Security Intelligence Service. The Canadian Security Intelligence Service (CSIS) is authorized to assist the ministers of National Defence and Foreign Affairs in collecting foreign intelligence within Canada. In carrying out its duties and functions, CSIS may, in turn, seek operational assistance and support from other departments and agencies, including CSE.

In 2002-03 my staff completed an examination of CSE's policies and practices in the context of a specific case where it provided operational support to CSIS. This examination found no evidence of unlawful activity on the part of CSE or any of its employees. Indeed, all the activities examined complied with CSE policies as well as relevant legal authorities.

My report did, however, make a number of recommendations designed to address weaknesses

in policy and practice that could lead to errors in handling sensitive information and to an inconsistent application of policy and law. CSE has started to take action to address the concerns I raised.

Information Technology Security. In earlier annual reports I discussed changes in the focus and complexity of activities undertaken by CSE under its Information Technology Security (ITS) program to protect government communications and communications systems. Among other things, the ITS program has shifted strategically toward a more open mode of doing business in the face of growing vulnerabilities as more and more government organizations adopt evolving technologies such as the Internet and electronic commerce.

To respond to a significantly expanded client base and greater demand for its services, the ITS program has actively sought cooperative partnerships and alliances with government and private sector organizations. These arrangements are usually formalized in written agreements between the parties. My Office reviewed formal agreements between the ITS program and external parties, as well as the policies, practices and procedures governing them, to identify issues and assess implications relating to lawfulness.

The review showed no evidence of unlawful activity on the part of CSE with respect to its arrangements with government and private sector organizations and the agreements arising from such arrangements. However, my report pointed to shortcomings in the administration of agreements as well as gaps in policy that created unnecessary risks in this regard. I have been informed that CSE is taking action to review and address my concerns and recommendations.

CSE's policies and procedures. One of my long-standing observations, based on several reviews carried out during my term as Commissioner, is that

CSE's internal policies and procedures have not always provided clear and consistent definitions and uses of key terms. I have found that policies and associated documentation were confusing at times, especially in instances where certain terms have multiple definitions.

As a follow-up to these observations, my staff compiled a lexicon of definitions of key terms from a number of different instruments, and I made that report available to the Minister and to CSE. In the course of this work, I learned that CSE is giving a high priority to the development and articulation of policies and procedures to guide operations under its mandate in the *National Defence Act*. This effort includes establishing new policies and procedures where necessary, as well as reviewing existing policies and procedures to ensure they are current and that they use accurate and consistent terminology.

I am encouraged by these developments at a time of expanded security and intelligence activity when, among other things, there are clear needs for CSE to retrain existing staff and to train and guide an anticipated influx of new employees. In these circumstances it is vitally important to ensure clear and consistent understanding and application of policy and procedures – including terminology used – throughout the organization. My Office will continue to monitor CSE's progress in this regard closely.

2002-03 Findings

Each year in this report I provide an overall statement on my findings about the lawfulness of CSE's activities based on the results of reviews my staff carried out during the year. Because of my new mandate under the *National Defence Act*, this is the first time my statement extends beyond lawfulness to compliance with ministerial authority.

I am able to report that the activities of CSE that my Office reviewed during the year complied with law and ministerial authority. In particular, while I found no evidence that CSE directed its activities at Canadians or any person in Canada, I did see evidence that CSE has measures to protect the privacy of Canadians in the use and retention of intercepted information.

Complaints and Concerns about CSE Activities

Paragraph 273.63 (2)(b) of the *National Defence Act* requires me, in response to a complaint, to undertake any investigation I consider necessary. During 2002-03, I received no complaints about CSE activities from any source.

Neither were concerns about CSE activities addressed to me under the public interest defence provisions of the *Security of Information Act*.

Review Agencies Conference

The third International Intelligence Review Agencies Conference was held in London, England, from 12-15 May 2002. Representatives of review agencies from Australia, Belgium, Canada, New Zealand, Poland, Slovakia, South Africa, and the United States met their United Kingdom counterparts to exchange views on issues of common interest in the historical setting of Lancaster House.

In addition to discussing review arrangements in our respective jurisdictions, we examined the issue of review from the perspectives of the agency being reviewed and the public, as well as in relation to changes in technology. I remain grateful to our hosts for their outstanding hospitality.

THE COMMISSIONER'S OFFICE

Office Expenditures and Staff

My budget allocation for the 2002-03 fiscal year was $921,950. Because the December 2001 amendments to the *National Defence Act* expanded my duties significantly, this allocation was 42 per cent greater than my budget in the previous year. The actual expenditures incurred in 2002-03 (see Annex B) were well within the budget.

During the year, my Office continued to consist of a small full-time staff. In addition, to help carry out my duties, I engaged the services of an independent legal counsel and several subject-matter experts on an ongoing basis.

Accommodation

My Office has occupied the same premises since my appointment in 1996, although by 1998 it was becoming evident that these premises offered insufficient accommodation for the staff and advisors I required to discharge my responsibilities. This situation became more acute following the additional responsibilities assigned to me by Parliament in late 2001.

In late 2002, I was advised that a larger office space was about to become available in the building that my Office has occupied since 1996. It was evident that this space would suit current requirements and also provide some flexibility for the future. My Office moved to its new location in May 2003.

LOOKING AHEAD

The Public Safety Act

In October 2002 the government introduced Bill C-17, the *Public Safety Act*, in Parliament. This bill, which replaced the earlier Bill C-55 (which in turn had replaced Bill C-42), was still under consideration as I was writing this report. Bill C-17 proposes legislative changes on a wide range of subjects, from transportation safety and immigration to biological weapons. Among the proposed changes are amendments to the *National Defence Act* that would confer significant new

responsibilities on the Commissioner of CSE for reviewing the lawfulness and compliance with ministerial authority of activities undertaken by the Department of National Defence or the Canadian Forces to protect their computer systems and networks, and for dealing with complaints arising from such activities.

I have informed the government of my concerns regarding the role proposed for the Commissioner in this Bill and its predecessors. Those concerns centre around the difficulties I can foresee in providing meaningful assurance of lawfulness and compliance with ministerial authority. In addition, however, I believe that assuming these new and potentially complex responsibilities would raise the question of whether the Commissioner's role could be carried out effectively on a part-time basis in the future.

In the meantime I have asked my officials to undertake a preliminary assessment of the review mandate envisaged in Bill C-17 so as to identify more clearly the systems that would be involved and the size of the sample of activities that would need to be reviewed for the Commissioner to give the assurances required. This will provide my successor with better information on the nature and extent of the work involved, and the possible impacts on this Office's resource requirements, should Parliament choose to confer these new duties on the Commissioner.

Appointment of a New Commissioner

My appointment as Commissioner expires on 19 June 2003.

Paragraph 273.63 (1) of the *National Defence Act* provides that the Governor in Council may appoint either a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment. However, I am concerned that a supernumerary judge would face serious limitations in carrying out the full range of duties and responsibilities involved.

These limitations arise from the blurring of lines between the executive and legislative arms of government on the one hand, and the judiciary on the other, that would result from appointing a supernumerary judge. For example, a supernumerary judge would not be in a position to comment on proposed legislation – as I have had occasion to do from time to time. Similarly, a supernumerary judge ought not to appear as a witness before parliamentary committees. Although I am somewhat disappointed not to have been called as a witness before parliamentary committees to discuss my annual reports, as a retired judge I would at least have been able to do so.

Regardless of the Governor in Council's decision, I wish my successor well in this fascinating and challenging assignment.

Concluding Thoughts

Finally, I would like to take this opportunity to say that serving Canada and Canadians during the past seven years has been a source of great and enduring satisfaction for me. I am convinced that through the very existence of this external review function, through the assurances that I have been able to provide and the opportunities for improvement that reviews have identified, my Office has made an important contribution to strengthening the control and accountability of CSE.

I would also like to say goodbye and to thank those I have worked with for seven years. In particular, the skill, dedication and unfailing good cheer of my staff have helped me immeasurably and have guided me through some challenging times. But I am also grateful for the respect and courtesy that CSE and other government officials have consistently extended to me and my staff. Their cooperation has made our task much easier.

Mandate of the Commissioner of the Communications Security Establishment

National Defence Act - Part V.1

"**273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

"**273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review."

Security of Information Act

"**15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

"**15.** (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

"**15.** (5) (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to,

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time."

Budget and Expenditures 2002-03

Expenditures

Salaries and Wages	201,935
Transportation and Telecommunications	21,808
Information	11,378
Professional and Special Services	209,699
Rentals	157,708
Purchased Repair and Maintenance	223,737
Materials and Supplies	4,438
Acquisition of Machinery and Equipment	26,098
Other Expenditures	22
Total	**$856,823**

Classified Reports, 1996-2003

Classified Report to the Minister – March 3, 1997 (TOP SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - February 6, 1998 (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister
- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister
- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- CSE's participation *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - August 21, 2002 (SECRET)

Classified Report to the Minister
- CSE's support to CSIS, as authorized by *** and code named *** - November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
- LEXICON - 26 March 2003 (TOP SECRET/COMINT)

Commissaire du Centre de la sécurité des télécommunications

Rapport annuel

2002
↓
2003

Canada

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2003
ISBN 0-662-67417-0
N° de cat. D95-2003

Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

Juin 2003

L'honorable John McCallum, C.P.
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2002-2003, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE DES MATIÈRES

Introduction 1

Évolution du rôle du commissaire 2

Activités de l'année 2002-2003 4

- Rapports classifiés 4
- Examens d'activités autorisées par le ministre 6
- Autres examens 8
- Constatations faites en 2002-2003 10
- Plaintes et préoccupations relatives aux activités du CST 11
- Conférence des organismes d'examen 11

Le bureau du commissaire 11

- Dépenses du bureau et personnel 11
- Locaux 12

Coup d'œil sur l'avenir 12

- La Loi sur la sécurité publique 12
- Nomination d'un nouveau commissaire 13
- Dernières réflexions 14

Annexe A : Mandat du commissaire 15

Annexe B : Budget et dépenses, 2002-2003 17

Annexe C : Rapports classifiés, 1996-2003 19

INTRODUCTION

Le présent rapport est mon septième à titre de commissaire du Centre de la sécurité des télécommunications (CST), et le dernier du fait que mon mandat prend fin en juin 2003. C'est par ailleurs la première fois, depuis ma nomination initiale en 1996, que j'ai examiné les activités du CST et rédigé mon rapport annuel dans le cadre d'une loi.

Je signalais dans mon dernier rapport qu'après plus d'une décennie de débats sur le pour et le contre d'une loi habilitante pour le CST, les tragiques événements du 11 septembre 2001 avaient précipité le dépôt et l'adoption par le Parlement de la loi omnibus intitulée *Loi antiterroriste*. Les modifications consécutives apportées à la *Loi sur la défense nationale*, entrées en vigueur le 24 décembre 2001, ont établi un mandat légal pour le CST et pour le commissaire. Les nouvelles dispositions de la *Loi sur la défense nationale* ont inscrit dans celle-ci les activités exercées depuis toujours par le CST et les fonctions que j'exerce depuis 1996, mais elles ont en outre instauré de nouveaux éléments. Ceux-ci sont décrits plus en détail dans la section suivante.

Évaluer les incidences de mes nouvelles responsabilités et commencer à satisfaire aux exigences de la loi ont absorbé une bonne partie de l'année écoulée. Celle-ci a donc été marquée par des défis et des changements tant pour le CST que pour mon bureau, alors que nous nous sommes efforcés d'arriver à une compréhension commune de nos rôles et responsabilités respectifs.

Dans le présent rapport, je fais une brève rétrospective de l'évolution et du développement du rôle du commissaire au cours des sept dernières années. Je rends également compte des activités d'examen et des constatations faites par mon bureau en 2002-2003. Celles-ci ont porté sur les deux principaux programmes du CST (renseignement

électromagnétique et sécurité des technologies de l'information) ainsi que sur certaines autres activités dont il s'acquitte. J'évoque enfin les faits nouveaux qui s'annoncent déjà, et la nomination de mon successeur.

ÉVOLUTION DU RÔLE DU COMMISSAIRE

Depuis mon entrée en fonction à titre de commissaire en 1996, le milieu très complexe dans lequel le CST exerce ses activités s'est considérablement transformé. Il en est allé de même de mon bureau et de ce que l'on attend de lui.

Un des aspects de ce changement touche le contexte à forte composante technologique dans lequel travaille le CST — et la technologie en cause a progressé à un rythme accéléré pendant toute cette période. Un autre élément clé concerne les modifications du contexte du renseignement découlant de l'évolution des réalités politiques, sociales et économiques. Celles-ci ont entraîné de nouvelles menaces pour la sécurité, la défense et les intérêts nationaux du Canada, et transformé les priorités gouvernementales en matière de renseignement. Pour faire face à ces défis, le CST a élargi son rôle en matière de collecte, d'analyse et de rapports de l'information et des renseignements. Mon personnel et moi-même avons dû nous familiariser avec les technologies complexes en cause et nous tenir au fait des changements rapides qui se produisaient afin de remplir les fonctions d'examen du commissaire d'une manière efficace et efficiente.

Tout au cours de cette période d'évolution technologique rapide qui a marqué le contexte du renseignement et les activités du CST, j'ai suivi le principe selon lequel les Canadiens doivent pouvoir compter que le CST, qui doit nécessairement effectuer la majorité de son travail en secret, le fait en conformité avec les lois du Canada. Ma responsabilité a consisté à leur donner cette assurance, et j'ai cherché à m'en acquitter en

maintenant l'ampleur, la profondeur et la crédibilité du travail d'examen de mon bureau et en mettant l'accent en particulier sur les questions qui pourraient mettre en danger la vie privée des Canadiens.

Le rôle du commissaire, tel qu'il s'était précisé dans les mandats établis dans les décrets de juin 1996 et de juin 1999 officialisant ma nomination, a été confirmé et élargi par le Parlement en décembre 2001, dans la *Loi antiterroriste*. L'élargissement le plus important découle des dispositions qui permettent au ministre de la Défense nationale d'autoriser l'interception par le CST des communications privées de Canadiens dans des circonstances particulières, sous réserve de l'observance de certaines conditions énoncées dans la loi[1]. L'article 183 du *Code criminel* définit une communication privée comme suit :

> Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers.

Ce nouveau pouvoir du CST d'intercepter des communications privées lorsque le ministre l'autorise à le faire est un fait nouveau important qui présente des risques manifestes pour la vie privée des Canadiens. La loi reconnaît ces risques et exige notamment que le ministre soit convaincu que le CST a mis en place des mesures adéquates pour protéger celle-ci. Elle prescrit en outre que le commissaire doit examiner les activités exercées en vertu de toutes les autorisations ministérielles pour s'assurer qu'elles sont effectivement autorisées, et

[1] Avant décembre 2001, le CST aurait enfreint les dispositions relatives à la vie privée tant du *Code criminel* que de la *Charte des droits et libertés* s'il avait intercepté des communications sans avoir la certitude que, ce faisant, il n'interceptait pas des communications privées.

qu'il fasse rapport annuellement de ces examens au ministre. En me fondant sur mon expérience jusqu'ici, je prévois qu'il s'agira là d'un aspect important et exigeant du rôle du commissaire à l'avenir.

Ce rôle a également été élargi par la *Loi sur la protection de l'information* (ancienne *Loi sur les secrets officiels*). Celle-ci interdit aux personnes astreintes au secret de communiquer ou de confirmer des « renseignements opérationnels spéciaux », y compris ceux qui ont trait aux activités du CST. Cependant, une personne ne sera pas reconnue coupable d'une infraction si elle peut établir qu'elle a agi dans l'intérêt public. Pour qu'un juge prenne en considération la « défense d'intérêt public », la personne en cause doit avoir pris une série de mesures prévues dans la loi avant de divulguer l'information. Ces mesures peuvent notamment consister à signaler ses préoccupations relatives aux activités du CST au commissaire et à lui donner un délai raisonnable pour y répondre. J'ai bon espoir que le commissaire sera rarement appelé à exercer ce rôle, mais celui-ci pourrait être important et risque d'être exigeant lorsque le cas se présentera.

On trouvera à l'annexe A les dispositions législatives stipulant le mandat du commissaire du Centre de la sécurité des télécommunications.

ACTIVITÉS DE L'ANNÉE 2002-2003

Rapports classifiés

Conformément aux décrets définissant mon mandat pour la période allant du 19 juin 1996 au 24 décembre 2001, mon bureau a effectué chaque année une série planifiée d'examens des activités du CST. Ces examens ont porté sur des domaines où, à mon avis, la nature même des activités du CST entraînait des risques liés à la légalité. Comme j'étais autorisé à présenter des rapports renfermant des renseignements classifiés au ministre de la Défense nationale chaque fois que je le jugeais à propos, j'ai pris l'habitude de rendre compte des

résultats de chacun de mes examens au ministre au moyen d'un rapport classifié.

La nouvelle loi a apporté certains changements importants à mon mandat. Comme je le mentionne plus haut, le ministre de la Défense nationale peut maintenant autoriser le CST à intercepter les communications privées de Canadiens dans certaines circonstances. Je suis toujours tenu d'examiner les activités du CST en général pour m'assurer qu'elles sont légales, mais la loi m'enjoint en outre expressément d'examiner les activités exercées par le CST en vertu d'autorisations ministérielles pour m'assurer que ces activités sont autorisées, et de faire rapport de cet examen au ministre annuellement.

Autrement dit, je n'ai plus toute latitude pour choisir les sujets d'examen. Mon nouveau mandat défini dans la loi ne m'autorise pas non plus expressément à présenter des rapports renfermant des renseignements classifiés au ministre chaque fois que je le juge à propos. Néanmoins, dans les cas où je choisis les sujets d'examen, j'estime sage de m'en tenir aux pratiques de rapport établies dans le cadre de mon mandat précédent, car elles m'ont bien servi par le passé.

Au cours de l'exercice 2002-2003, j'ai adressé quatre rapports classifiés au ministre, et un autre était presque achevé à la fin de l'année. Il s'agit notamment de rapports exigés par la nouvelle loi et d'examens dont j'avais choisi le sujet. L'annexe C renferme la liste de tous les rapports classifiés que j'ai adressés au ministre depuis ma nomination en 1996.

Comme je l'ai fait remarquer par le passé, la présentation d'un rapport classifié au ministre ne signifie pas que j'aie décelé un manque quelconque de conformité à la loi ou à une autorisation ministérielle. Cela indique simplement que le

rapport contient des documents qui nécessitent ce traitement. De fait, je suis heureux de pouvoir dire qu'aucun des examens qui ont formé la base de mes 23 rapports classifiés (y compris les quatre présentés en 2002-2003) n'a fait ressortir de cas d'illégalité ou d'activité non autorisée.

Examens d'activités autorisées par le ministre

Conformément aux paragraphes 273.65 (1) et (3) de la *Loi sur la défense nationale*, le ministre de la Défense nationale a autorisé par écrit le CST à intercepter des communications privées aux fins d'obtenir des renseignements étrangers et de protéger les systèmes ou les réseaux informatiques de l'État de tout méfait, utilisation non autorisée ou perturbation de leur fonctionnement. Comme nombre des activités exercées en vertu de ces autorisations étaient nouvelles pour le CST, elles ont suscité des défis importants touchant non seulement la technologie, mais aussi des questions comme la détermination des rôles et responsabilités appropriés, l'élaboration d'une politique et de procédures destinées à guider les activités, et l'élaboration de mesures de contrôle afin de garantir le respect des conditions imposées par la loi et par les autorisations ministérielles. Le CST continue de relever ces défis.

L'information fournie par le CST montre que la majeure partie des communications interceptées en vertu de ces autorisations ne sont en fait pas privées (c'est-à-dire qu'il ne s'agit pas de communications de Canadiens). Or je pense que mon examen doit porter uniquement sur les communications privées. Quelles que soient les autres communications interceptées par le CST, c'est l'interception de communications privées qui est autorisée expressément par le ministre. De plus, c'est en ce qui concerne l'interception, l'utilisation et la conservation de communications privées que les questions de légalité et de conformité à l'autorité ministérielle sont le plus susceptibles de se poser.

En conséquence, au cours de l'année écoulée, mon bureau a consacré une bonne partie de ses activités à examiner comment le CST acquiert et reconnaît ces communications, comment il y accède, comment il les conserve et les utilise, et quel genre de politique, de procédures et de cadre de contrôle de la gestion il met en place. Pour ce faire, mon personnel et moi-même avons examiné une certaine quantité de documents et de correspondance, eu plusieurs entretiens avec des représentants du CST et assisté à des breffages et des séances d'information. J'ai en outre demandé au CST de me décrire une mission précise effectuée en vertu de l'une des autorisations.

Mon bureau a effectué un examen préliminaire d'activités menées conformément à une autorisation ministérielle. En vertu de celle-ci, le CST était autorisé à mener, à partir du Canada, des activités relatives à l'interception de communications dans le seul but d'obtenir des renseignements étrangers et, ce faisant, d'intercepter des communications privées sous réserve des conditions définies dans la loi et dans l'autorisation ministérielle. Comme l'exige la loi, j'ai fait rapport au ministre des constatations issues de cet examen préliminaire. En raison de l'objet de l'autorisation ministérielle, et parce que cet examen était une première pour mon bureau, mon rapport préliminaire a porté davantage sur le processus et la classe d'activités autorisées que sur la conformité du CST à l'autorisation. Je prévois que, dans les rapports annuels futurs qu'il adressera au ministre en vertu de l'article 273.65 de la partie V.1 de la *Loi sur la défense nationale*, le commissaire sera en mesure de traiter plus directement des questions de conformité.

Mes examens des activités entreprises en vertu d'autres autorisations ministérielles en vigueur au cours de l'exercice 2002-2003 étaient en cours à la fin de l'année et feront l'objet de rapports au ministre dans le proche avenir.

Autres examens

Soutien opérationnel apporté par le CST au Service canadien du renseignement de sécurité. Le Service canadien du renseignement de sécurité (SCRS) est autorisé à aider le ministre de la Défense nationale et le ministre des Affaires étrangères à recueillir des renseignements étrangers au Canada. Dans l'exercice de ses fonctions et responsabilités, le SCRS peut également solliciter l'aide et le soutien opérationnels d'autres ministères et organismes, dont le CST.

En 2002-2003, mon personnel a effectué un examen des politiques et pratiques du CST dans le contexte d'un cas précis où celui-ci a apporté un soutien opérationnel au SCRS. Cet examen n'a fait ressortir aucune preuve d'activité illégale de la part du CST ni d'aucun de ses employés. En effet, toutes les activités examinées étaient conformes aux politiques de l'organisme ainsi qu'aux autorisations légales pertinentes.

Mon rapport contenait cependant un certain nombre de recommandations destinées à remédier à des faiblesses de la politique et de la pratique qui pourraient entraîner des erreurs de traitement de renseignements délicats, et à un manque d'uniformité dans l'application de la politique et de la loi. Le CST a commencé à prendre des mesures pour répondre aux préoccupations que j'ai soulevées.

Sécurité des technologies de l'information. J'ai traité dans des rapports annuels antérieurs des modifications de l'objet et de la complexité des activités menées par le CST dans le cadre de son programme de sécurité des technologies de l'information (STI) afin de protéger les communications et les systèmes de communication du gouvernement. Le programme de STI s'est entre autres réorienté stratégiquement dans le sens d'une plus grande ouverture face aux vulnérabilités qui augmentent à mesure qu'un plus grand nombre d'organisations gouvernementales adoptent des technologies nouvelles comme Internet et le commerce électronique.

Compte tenu d'une augmentation considérable de sa clientèle et d'un accroissement de la demande visant ses services, le programme de STI a cherché activement à former des partenariats et des alliances avec des organismes du gouvernement et du secteur privé. Ces arrangements sont habituellement officialisés par des ententes écrites entre les parties. Mon bureau a examiné les ententes officielles entre le programme de STI et des organismes externes, ainsi que les politiques, les pratiques et les procédures qui les régissent, afin de repérer d'éventuels problèmes et d'en évaluer l'incidence sous le rapport de la légalité.

Cet examen n'a révélé aucun indice d'activité illégale de la part du CST touchant ses arrangements avec des organismes du gouvernement et du secteur privé et les ententes en découlant. Toutefois, mon rapport a souligné des défauts dans l'administration des ententes ainsi que des lacunes de politique qui créent des risques inutiles à cet égard. On m'informe que le CST prend des mesures pour étudier mes préoccupations et mes recommandations et pour y donner suite.

Politiques et procédures du CST. L'une de mes observations de longue date, qui se fonde sur plusieurs examens effectués au cours de mon mandat, est que les politiques et les procédures internes du CST n'ont pas toujours fourni des définitions et des emplois clairs et uniformes de termes clés. J'ai constaté que les politiques et la documentation connexe étaient parfois déroutantes, en particulier lorsque certains termes ont de multiples définitions.

À la suite de ces observations, mon personnel a dressé un lexique de termes clés à partir de plusieurs outils, et j'ai communiqué ce rapport au ministre et au CST. Au cours de ce travail, j'ai appris que le CST considérait comme hautement prioritaires l'élaboration et la formulation de

politiques et de procédures destinées à guider les opérations découlant de son mandat énoncé dans la *Loi sur la défense nationale*. Cette entreprise comprend l'établissement de politiques et de procédures nouvelles, là où c'est nécessaire, ainsi que l'examen des politiques et des procédures existantes pour s'assurer qu'elles sont d'actualité et qu'elles emploient une terminologie exacte et uniforme.

Je suis encouragé par cette évolution à un moment où les activités de sécurité et de renseignement sont en plein essor et où il est évident que le CST doit assurer le perfectionnement de son personnel en place, en plus de former et de guider une future cohorte de nouveaux employés. Dans ces circonstances, il est capital d'assurer la compréhension et l'application claires et uniformes de la politique et des procédures – y compris la terminologie employée – à l'échelle de l'organisme. Mon bureau continuera de suivre de près les progrès accomplis par le CST à cet égard.

Constatations faites en 2002-2003

Je fournis comme chaque année dans le présent rapport un énoncé global de mes constatations au sujet de la légalité des activités du CST, en me fondant sur les résultats des examens effectués par mon personnel pendant l'année. Compte tenu de mon nouveau mandat en vertu de la *Loi sur la défense nationale*, cet énoncé va pour la première fois au-delà de la légalité pour englober la conformité à l'autorisation ministérielle.

Je suis à même de signaler que les activités du CST que mon bureau a examinées au cours de l'année étaient conformes à la loi et à l'autorisation ministérielle. Ainsi, je n'ai trouvé aucun indice révélant que les activités du CST visaient des Canadiens ou d'autres personnes au Canada, mais j'ai vu des preuves des mesures mises en place par le CST pour protéger la vie privée des Canadiens en ce qui touche l'utilisation et la conservation des renseignements interceptés.

Plaintes et préoccupations relatives aux activités du CST

L'alinéa 273.63 (2)b) de la *Loi sur la défense nationale* m'oblige à effectuer toute enquête que je juge nécessaire à la suite d'une plainte. Au cours de l'année 2002-2003, je n'ai reçu aucune plainte de quelque source que ce soit au sujet des activités du CST.

On ne m'a pas non plus signalé de préoccupations au sujet des activités du CST en vertu des dispositions de la *Loi sur la protection de l'information* portant sur la défense d'intérêt public.

Conférence des organismes d'examen

La troisième conférence internationale des organismes d'examen des activités de renseignement s'est tenue à Londres, en Angleterre, du 12 au 15 mai 2002. Des représentants de l'Afrique du Sud, de l'Australie, de la Belgique, du Canada, des États-Unis, de la Nouvelle-Zélande, de la Pologne et de la Slovaquie ont rencontré leurs homologues du Royaume-Uni pour discuter de questions d'intérêt commun, dans le cadre historique de Lancaster House.

Outre les modalités d'examen dans nos pays respectifs, nous avons examiné la question de l'examen du point de vue de l'organisme visé et du public, ainsi que par rapport à l'évolution de la technologie. Je suis reconnaissant à nos hôtes de leur généreuse hospitalité.

LE BUREAU DU COMMISSAIRE

Dépenses du bureau et personnel

Le budget qui m'avait été alloué pour l'année financière 2002-2003 était de 921 950 $. Comme les modifications apportées à la *Loi sur la défense nationale* en décembre 2001 avaient sensiblement élargi mes fonctions, ce budget dépassait celui de l'année précédente de 42 p. 100. Les dépenses engagées en 2002-2003 (voir l'annexe B) sont restées bien en deçà de ce budget.

Au cours de l'année, mon bureau a continué de se composer d'un petit noyau de personnel à plein

temps. J'ai par ailleurs retenu les services d'un conseiller juridique indépendant et de plusieurs spécialistes de questions particulières sur une base régulière pour m'aider à m'acquitter de mes fonctions.

Locaux

Mon bureau est situé dans les mêmes locaux depuis ma nomination, en 1996, même si, dès 1998, il est devenu évident que ceux-ci étaient insuffisants pour loger le personnel et les conseillers dont j'ai besoin pour m'acquitter de mes responsabilités. Cette situation est devenue plus critique après que le Parlement m'a confié de nouvelles responsabilités, à la fin de 2001.

À la fin de 2002, on m'a informé que des locaux plus spacieux étaient sur le point de se libérer dans l'immeuble où se trouve mon bureau depuis 1996. Il était évident que cet espace répondrait aux besoins actuels et assurerait une certaine souplesse pour l'avenir. Nous avons emménagé dans ces nouveaux locaux en mai 2003.

COUP D'ŒIL SUR L'AVENIR

La Loi sur la sécurité publique

En octobre 2002, le gouvernement a déposé au Parlement le projet de loi C-17, *Loi sur la sécurité publique*. Celui-ci, qui a remplacé le projet de loi C-55, déposé antérieurement (et qui avait lui-même remplacé le projet de loi C-42), était encore à l'étude au Parlement au moment de la rédaction du présent rapport. Le projet de loi C-17 propose des modifications législatives touchant un grand nombre de sujets, de la sécurité des transports à l'immigration en passant par les armes biologiques. Parmi celles-ci figurent des modifications de la *Loi sur la défense nationale* qui conféreraient de nouvelles responsabilités importantes au commissaire du CST touchant l'examen de la légalité et de la conformité à l'autorisation ministérielle des activités entreprises par le ministère de la Défense nationale ou par les Forces canadiennes afin de protéger leurs systèmes et

réseaux informatiques, et le traitement des plaintes découlant de ces activités.

J'ai informé le gouvernement de mes préoccupations au sujet du rôle proposé pour le commissaire dans ce projet de loi et ceux qui l'ont précédé. Ces préoccupations ont trait aux difficultés que j'entrevois lorsqu'il s'agirait de fournir une garantie sérieuse de légalité et de conformité à l'autorité ministérielle. J'estime en outre que la prise en charge de ces responsabilités nouvelles et susceptibles d'être complexes soulèverait la question de savoir si les fonctions du commissaire pourraient à l'avenir être exercées à temps partiel.

Entre-temps, j'ai demandé à mes fonctionnaires de procéder à une évaluation préliminaire du mandat d'examen envisagé dans le projet de loi C-17, afin de définir plus clairement les systèmes qui seraient en cause et la taille de l'échantillon d'activités qui devrait être examiné pour permettre au commissaire de donner les assurances requises. Cela fournira à mon successeur une meilleure information sur la nature et l'ampleur du travail, et sur ses répercussions possibles sur les ressources nécessaires au bureau du commissaire, si le Parlement décide de lui confier ces nouvelles fonctions.

Nomination d'un nouveau commissaire

Mon mandat à titre de commissaire expire le 19 juin 2003.

Le paragraphe 273.63 (1) de la *Loi sur la défense nationale* prévoit que le gouverneur en conseil peut nommer soit un juge surnuméraire, soit un juge d'une cour supérieure à la retraite au poste de commissaire du Centre de la sécurité des télécommunications. Toutefois, je m'inquiète du fait qu'un juge surnuméraire ferait face à des limites sérieuses pour ce qui est de remplir l'ensemble des fonctions et des responsabilités du poste.

Ces limites tiennent au fait que la nomination d'un juge surnuméraire estomperait la démarcation entre les pouvoirs exécutif et législatif, d'une part, et le pouvoir judiciaire, de l'autre. Par exemple, un juge surnuméraire ne serait pas en mesure de commenter des projets de loi, comme j'ai eu l'occasion de le faire de temps à autre. De même, il ne devrait pas comparaître devant des comités parlementaires. Si je suis quelque peu déçu de ne pas avoir été appelé à témoigner devant des comités parlementaires pour discuter de mes rapports annuels, en ma qualité de juge à la retraite, j'aurais au moins pu le faire.

Mais quelle que soit la décision du gouverneur en conseil, je souhaite à celui ou celle qui prendra la relève un franc succès dans cette mission passionnante et exigeante.

Dernières réflexions

Enfin, j'aimerais profiter de l'occasion pour dire que mon travail au service du Canada et des Canadiens au cours des sept dernières années a été pour moi une source de profonde et durable satisfaction. Je suis convaincu que, grâce à l'existence même de cette fonction d'examen externe, grâce aux assurances que j'ai pu fournir et aux possibilités d'amélioration que les examens ont fait ressortir, mon bureau a fourni un apport important au renforcement du contrôle et de la responsabilité du CST.

J'aimerais par ailleurs saluer et remercier les personnes avec qui j'ai travaillé pendant sept ans. La compétence, le dévouement et la bonne humeur indéfectible de mon personnel m'ont été d'une aide inestimable et m'ont guidé dans des moments difficiles. Je suis également reconnaissant du respect et de la courtoisie que le CST et les autres fonctionnaires de l'État nous ont toujours témoignés, à mon personnel et à moi-même. Leur coopération a grandement facilité notre tâche.

Mandat du commissaire du Centre de la sécurité des télécommunications

Loi sur la défense nationale - Partie V.1

« **273.63** (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

« **273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

Loi sur la protection de l'information

« **15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« **15.** (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« **15.** (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »

Budget et dépenses, 2002-2003

Dépenses

Traitements et salaires	201 935
Transports et télécommunications	21 808
Information	11 378
Services professionnels et spéciaux	209 699
Location	157 708
Achat de services de réparation et d'entretien	223 737
Fournitures et approvisionnements	4 438
Acquisition de machine et de matériel	26 098
Autres charges	22
Total	**856 824 $**

Rapports classifiés, 1996-2003

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
CSE's participation *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - 20 août 2002 (SECRET)

Classified Report to the Minister
- CSE's support to CSIS, as authorized by *** and code named *** - 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister

- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization - 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister

- LEXICON - 26 mars 2003 (TRÈS SECRET/COMINT)